CLAIMS

What is claimed is:

Sub a1

1. A method comprising:

writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document;

signing the electronic document to obtain a once signed electronic document; and

transmitting the once signed electronic document to a second digital certificate issuing authority to obtain a twice signed electronic document.

2. The method of claim 1 wherein signing the electronic document to obtain a once signed electronic document comprises:

obtaining a hash value using contents of the electronic document as input to a hash algorithm;

encrypting the hash value using the first digital certificate issuing authority's private key; and

storing the encrypted hash value in the electronic document.

3. The method of claim 1 wherein obtaining a twice signed electronic document comprises at least one of the second digital certificate issuing authority inserting its authenticating information in the once signed electronic document, obtaining a hash value using contents of the electronic document as input to a hash algorithm, encrypting the

hash value using the second digital certificate issuing authority's private key, including the encrypted hash value in the electronic document, and transmitting the twice signed electronic document.

4. The method of claim 3 wherein obtaining a hash value using contents of the electronic document as input to a hash algorithm comprises at least one of, using the party's authenticating information, using the first digital certificate issuing authority's authenticating information, using the digital signature of the first digital certificate issuing authority, and using the second digital certificate issuing authority's authenticating information as input to a hash algorithm.

5. The method of claim 1, wherein writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document comprises receiving the party's authenticating information via a secure connection.

6. A computer system comprising:

a bus;

a data storage device coupled to said bus; and

a processor coupled to said data storage device, said processor operable to receive instructions which, when executed by the processor, cause the processor to perform a method comprising writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document;

signing the electronic document to obtain a once signed electronic document; and

transmitting the once signed electronic document to a second digital certificate issuing authority to obtain a twice signed electronic document.

7. A computer system as in claim 6 wherein signing the electronic document to obtain a once signed electronic document comprises:

obtaining a hash value using contents of the electronic document as input to a hash algorithm;

encrypting the hash value using the first digital certificate issuing authority's private key; and

storing the encrypted hash value in the electronic document.

8. A computer system as in claim 6 wherein obtaining a twice signed electronic document comprises at least one of the second digital certificate issuing authority inserting its authenticating information in the once signed electronic document, obtaining a hash value using contents of the electronic document as input to a hash algorithm, encrypting the hash value using the second digital certificate issuing authority's private key, including the encrypted hash value in the electronic document, and transmitting the twice signed electronic document.

9. A computer system as in claim 8 wherein obtaining a hash value using contents of the electronic document as input to a hash algorithm comprises at least one of, using the party's authenticating information, using the first digital certificate issuing authority's

authenticating information, using the digital signature of the first digital certificate issuing authority, and using the second digital certificate issuing authority's authenticating information as input to a hash algorithm.

10. A computer system as in claim 6 wherein writing a party's authenticating information and a first digital certificate issuing authorities authenticating information in an electronic document comprises receiving the party's authenticating information via a secure connection.

11. An article of manufacture comprising:

a machine-accessible medium including instructions that, when executed by a machine, causes the machine to perform operations comprising

writing a party's authenticating information and a first digital certificate issuing authorities authenticating information in an electronic document;

signing the electronic document to obtain a once signed electronic document; and

transmitting the once signed electronic document to a second digital certificate issuing authority to obtain a twice signed electronic document.

12. An article of manufacture as in claim 11 wherein signing the electronic document to obtain a once signed electronic document comprises:

obtaining a hash value using contents of the electronic document as input to a hash algorithm;

encrypting the hash value using the first digital certificate issuing authority's private key; and

storing the encrypted hash value in the electronic document.

13. An article of manufacture as in claim 11 wherein obtaining a twice signed electronic document comprises at least one of the second digital certificate issuing authority inserting its authenticating information in the once signed electronic document, obtaining a hash value using contents of the electronic document as input to a hash algorithm, encrypting the hash value using the second digital certificate issuing authority's private key, including the encrypted hash value in the electronic document, and transmitting the twice signed electronic document.

14. An article of manufacture as in claim 13 wherein obtaining a hash value using contents of the electronic document as input to a hash algorithm comprises at least one of, using the party's authenticating information, using the first digital certificate issuing authorities authenticating information, using the digital signature of the first digital certificate issuing authority, and using the second digital certificate issuing authority's authenticating information as input to a hash algorithm.

15. An article of manufacture as in claim 11 wherein writing a party's authenticating information and a first digital certificate issuing authorities authenticating information in an electronic document comprises receiving the party's authenticating information via a secure connection.

16. A method comprising:
receiving a once signed electronic document;
writing a digital certificate issuing authority's authenticating information in the once signed electronic document;
signing the once signed electronic document to form a twice signed electronic document; and
transmitting the twice signed electronic document.

17. The method of claim 16 wherein signing the once signed electronic document to form a twice signed electronic document comprises:

obtaining a hash value using contents of the once signed electronic document and using the digital certificate issuing authority's authenticating information as input to a hash algorithm;

encrypting the hash value using the digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

18. A computer system comprising:
a bus;
a data storage device coupled to said bus; and
a processor coupled to said data storage device, said processor operable to receive instructions which, when executed by the processor, cause the processor to perform a method comprising receiving a once signed electronic document;

writing a digital certificate issuing authority's authenticating information in the once signed electronic document;

signing the once signed electronic document to form a twice signed electronic document; and

transmitting the twice signed electronic document.

19. A computer system as in claim 18 wherein signing the once signed electronic document to form a twice signed electronic document comprises:

obtaining a hash value using contents of the once signed electronic document and using the digital certificate issuing authority's authenticating information as input to a hash algorithm;

encrypting the hash value using the digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

20. An article of manufacture comprising:

a machine-accessible medium including instructions that, when executed by a machine, causes the machine to perform operations comprising receiving a once signed electronic document;

writing a digital certificate issuing authority's authenticating information in the once signed electronic document;

signing the once signed electronic document to form a twice signed electronic document; and transmitting the twice signed electronic document.

21. An article of manufacture as in claim 20 wherein signing the once signed electronic document to form a twice signed electronic document comprises:

obtaining a hash value using contents of the once signed electronic document and using the digital certificate issuing authority's authenticating information as input to a hash algorithm;

encrypting the hash value using the digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.